DIGIMARC

9405 SW Gemini Drive, Beaverton, OR 97008 USA
T. +1 503.469.4800 F. +1 503.469.4777 www.digimarc.com

FACSIMILE TRANSMITTAL

DATE: November 29, 2005

TO: Commissioner of Patents

FAX: 571-273-8300

FROM: Steven W. Stewart

PAGES: 26 (including cover)

RE: U.S. Patent Application No. 09/864,084

FILED: May 22, 2001

FOR: DIGITAL WATERMARKING APPARATUS, SYSTEMS AND METHODS

ART UNIT: 2132

DOCKET NO.: P0377

✓ Urgent ☐ For Review ☐ Please Reply

FACSIMILE COVER LETTER

Attached are an Appeal Brief and Transmittal Letter with deposit account authorization for the above referenced application.

CERTIFICATE OF FAXING

I hereby certify that these papers are being facsimile transmitted to the US Patent Office, 571-273-8300 on November 29, 2005.

Steven W. Stewart, Reg. No. 45,133
Attorney for Applicant

If you do not receive all pages or if you have problems receiving transmittal, please call us at 503-469-4800.

SWS:lmp 11/29/05 P0377

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Response Under 37 CFR § 1.116
Expedited Procedure

In re application of:

Phillip Andrew Seder

Application No.: **09/864,084**

Filed: May 22, 2001

For: DIGITAL WATERMARKING APPARATUS, SYSTEMS AND METHODS

Examiner: S. Lemma

Date: November 29, 2005

Art Unit 2132
Confirmation No. 1802

CERTIFICATE OF TRANSMISSION

I hereby certify that this paper and the documents referred to as being attached or enclosed herewith are being facsimile transmitted to the United States Patent and Trademark Office at 571-273-8300 on November 29, 2005.

Steven W. Stewart
Attorney for Applicants

TRANSMITTAL LETTER

MAIL STOP APPEAL BRIEF – PATENTS
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Enclosed for filing in the above-captioned matter are the following:

☒ Appeal Brief (fee **$500.00**)

☒ Applicant petitions for a one (1) month extension of time from October 29, 2005 to November 29, 2005 (fee **$120.00**).

☒ Please charge **$620.00** (fee for Appeal Brief and Extension of time) and any additional fees which may be required in connection with filing this document and any extension of time fee, or credit any overpayment, to Deposit Account No. 50-1071.

Date: November 29, 2005

CUSTOMER NUMBER 23735

Phone: 503-469-4800
FAX 503-469-4777

Respectfully submitted,

DIGIMARC CORPORATION

By

Steven W. Stewart
Registration No. 45,133

12/01/2005 MBINAS 00000013 501071 09864084
01 FC:1251 120.00 DA

SWS:lmp 11/29/05 P0377

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Phillip Andrew Seder

Application No.: **09/864,084**

Filed: May 22, 2001

For: DIGITAL WATERMARKING APPARATUS, SYSTEMS AND METHODS

Examiner: S. LEMMA

Date: November 29, 2005

Response Under 37 CFR § 1.116

Expedited Procedure

Art Unit: 2132

Confirmation No.: 1802

CERTIFICATE OF TRANSMISSION

I hereby certify that this paper and the documents referred to as being attached or enclosed herewith are being facsimile transmitted to the United States Patent and Trademark Office at 571-273-8300 on November 29, 2005.

Steven W. Stewart
Attorney for Applicants

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Appellants respectfully request the Board of Patent Appeals and Interferences (hereafter referred to as "the Board") to reverse the outstanding final rejection of the pending claims.

This Appeal Brief is in furtherance of a Notice of Appeal filed August 29, 2005 (postcard stamped September 1, 2005). Please charge the fee required under 37 CFR 1.17(f) or any needed fee to deposit account 50-1071.

12/01/2005 MBINAS 00000013 501071 09864084
02 FC:1402 500.00 DA

REAL PARTY IN INTEREST

The real party in interest is Digimarc Corporation, by an assignment from the inventors recorded at Reel 012193, Frames 0201-0202, on September 24, 2001.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

Claims 1-4, 8-17, 19-29 and 31-38 are pending in the present application. (Claims 5-7, 18 and 30 have been previously canceled.) Each of the pending claims stand finally rejected. *Please see* the Office Action Summary in the final Office Action mailed June 2, 2005.

STATUS OF AMENDMENTS

All earlier-filed amendments have been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

By way of general background, embedded machine-readable code can be used to link to or otherwise identify related information. In one illustrative example, a document or object is embedded with an identifier (or machine readable code). The identifier is extracted by a reading device and is passed to a computer server. The computer server includes (or communicates with) a database with related information (or "pointers"). The related information is indexed via identifiers. Such related information or pointers may include a URL, web address, IP address, and/or other information. An extracted identifier is used to interrogate the database to locate corresponding related information, such as a URL. The URL is passed from the computer server to the reading device, which directs a web browser with the URL. *Please see, e.g.*, paragraph 13 on page 3 of the specification.

By way of additional background, an enhancement can be made to the above systems and methods. Consider an example where a URL points to confidential material, or to a privileged

website (e.g., a website accessible through watermarked documents, secret, etc.). In this case, it might be advantageous to restrict access to the corresponding website, allowing access to only those users having physical possession of a corresponding watermarked or encoded document or object. Accordingly, there was a need for a verification system for use with watermark-based (or identifier-based) routing to websites, files, databases, networks, computers, etc. *Please see, e.g.*, paragraph 14 on page 3 of the specification.

Accordingly, one implementation of the invention, as recited in claim 10, is a method of authenticating permission to access a system. The method includes: receiving a request to enter the system (see, e.g., page 16, lines 1-3 of paragraph 60, see also Fig. 11), the request including at least a validation key (see, e.g., page 16, lines 1-3 of paragraph 60); determining whether the validation key is valid, wherein the validation key comprises a time stamp and said determining determines whether the time stamp comprises a predetermined format (see, e.g., page 16, lines 4-10 of paragraph 60, see also Fig. 11); and allowing access to the system based on a determination of said determining (see, e.g., page 16, lines 10-12 of paragraph 60, see also Fig. 11).

Another implementation of the invention, as recited in claim 20, is a method of authenticating permission to access a system via the internet. The method includes: receiving a request to enter the system, the request including at least a validation key (see, e.g., page 16, lines 1-3 of paragraph 61); determining whether the validation key has been previously received (see, e.g., page 16, lines 1-3 of paragraph 61, see also Fig. 12); and allowing access to the system based on a determination of said determining (see, e.g., page 17, lines 4-6 of paragraph 61, see also Fig. 12).

Yet another implementation of the invention, as recited in claim 24, is a system for exchanging data. The system (see, e.g., component of Fig. 7) includes: a central server (see, e.g., Fig. 7, reference no. 18) comprising at least one database including pointer information (see, e.g., page 12, lines 1-3 of paragraph 47), wherein when a user terminal (see, e.g., Fig. 7, reference no. 16) communicates an extracted watermark identifier to said central server (see, e.g., page 11, lines 2-6 of paragraph 46), said central server identifies a corresponding pointer associated with the extracted watermark identifier (see, e.g., page 12, lines 1-3 of paragraph 47), and wherein

said central server generates a validation key including at least one of a random and pseudo-random number (see, e.g., page 12, lines 1-2 of paragraph 49; see also original claim 30 on page 23 of the originally filed specification), and encodes the validation key (see, e.g., pages 12-13, lines 8-17 of paragraph 49; see also page 12, lines 5-6 of paragraph 47), and wherein said central server appends the validation key to the corresponding pointer (see, e.g., page 14, lines 1-2 of paragraph 54), and communicates the pointer and validation key to the user terminal (see, e.g., page 14, lines 1-2 of paragraph 54).

Still another implementation of the invention, as recited in claim 31, is a method of operating a computer server. The computer server communicates with at least one user terminal. The method includes: receiving an identifier from the user terminal (see, e.g., page 12, lines 1-2 of paragraph 47); identifying a pointer associated with the identifier (see, e.g., page 12, lines 1-3 of paragraph 47; see also Fig. 8); determining whether the pointer is a predetermined class (see, e.g., page 12, lines 3-4 of paragraph 47; see also Fig. 8), and if not the predetermined class, communicating the pointer to the user terminal (see, e.g., page 12, lines 4-5 of paragraph 47; see also Fig. 8); and if the predetermined class, generating a validation key, and communicating the pointer and validation key to the user terminal (see, e.g., page 12, lines 5-7 of paragraph 47; see also Fig. 8).

Yet another implementation of the invention, as recited in claim 38, is a computer server. The computer server is to communicate with at least one user terminal. The server includes: means for receiving (e.g., page 19, paragraph 73; see also reference no. 18, Fig. 7) an identifier from the user terminal (see, e.g., page 12, lines 1-2 of paragraph 47); means for identifying (e.g., page 19, paragraph 73, see also reference no. 18, Fig. 7) a pointer associated with the identifier (see, e.g., page 12, lines 1-3 of paragraph 47; see also Fig. 8); means for determining (e.g., page 19, paragraph 73, see also reference no. 18, Fig. 7) whether the pointer is a predetermined class (see, e.g., page 12, lines 3-4 of paragraph 47; see also Fig. 8), and if not the predetermined class, means for communicating (e.g., page 19, paragraph 73, see also reference no. 18, Fig. 7) the pointer to the user terminal (see, e.g., page 12, lines 4-5 of paragraph 47; see also Fig. 8); and if the predetermined class, means for generating (e.g., page 19, paragraph 73, see also reference no.

18, Fig. 7) a validation key, and communicating the pointer and validation key to the user terminal (see, e.g., page 12, lines 5-7 of paragraph 47; see also Fig. 8).

Still another implementation, as recited in claim 1, is a method of regulating access to a website (see, e.g., Fig. 7, item 20) by a user terminal (see, e.g., Fig. 7, item 16) via the internet (see, e.g., Fig. 7, item 22). The user terminal (see, e.g., Fig. 7, item 16) reads a document (see, e.g., Fig. 7, item 12) including an embedded digital watermark (see, e.g., page 11, paragraph 46). The method includes: at the user terminal (see, e.g., Fig. 7, item 16), extracting identifying data from the digital watermark (see, e.g., page 11, paragraph 46), and providing the identifying data to a central computer (see, e.g., Fig. 7, item 18; see also page 11, paragraph 46); at the central computer: identifying a pointer associated with the identifying data (see, e.g., page 12, paragraph 47); generating a validation key (see, e.g., page 12, paragraphs 47 and 49); encoding the validation key through at least one of i) hashing (see, e.g., page 12, lines 9-11 of paragraph 49), ii) rotating (see, e.g., page 13, paragraph 50) and iii) converting the validation key to alpha-characters and then adjusting the characters according to a code key (see, e.g., page 13, paragraph 50); and providing the pointer and the validation key to the user terminal (see, e.g., page 14, paragraph 54); at the user terminal (see, e.g., Fig. 7, item 16), communicating with the website (see, e.g., Fig. 7, item 20) via the pointer and providing the validation key to the website (see, e.g., Fig. 7, item 20; see also page 14-15, paragraph 55); and at the website, regulating access to the website by the user terminal based at least in part on the validation key (see, e.g., pages 15-16, paragraphs 56-59).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-4, 8-17, 19-29 and 31-38 stand finally rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,631,404 (hereafter referred to as "the Philyaw patent").

ARGUMENT

Appellants respectfully request that the final rejection of the pending claims be reversed since the cited references fail to teach or suggest all of the elements of the pending claims.

Rejections under U.S.C. 102(e) over the Philyaw Patent

Claims 24 - 29

Independent claim 24 recites the following:

24. A system for exchanging data comprising:

a central server comprising at least one database including pointer information, wherein when a user terminal communicates an extracted watermark identifier to said central server, said central server identifies a corresponding pointer associated with the extracted watermark identifier, and wherein said central server generates a validation key including at least one of a random and pseudo-random number, and encodes the validation key, and wherein said central server appends the validation key to the corresponding pointer, and communicates the pointer and validation key to the user terminal.

We have carefully studied the cited[1] passage of the Philyaw patent and do not see any mention of a "random" or "pseudo-random" number, let alone a validation key including such. We have even performed a word search of the entire Philyaw patent via the United States Patent

---

1 See the final Office Action on page 6, lines 12 -- page 7, lines 4, citing the Philyaw patent at Col. 29, lines 35-63

and Trademark Office website. Moreover, there does **not** appear to be **any** mention of the term random or pseudo-random in the Philyaw patent at all.

In view of this we believed that the Examiner has mischaracterized the cited passages of the Philyaw patent in the final Office Action on page 6, line 12 – page 7, line 4.

Moreover, discussion of users being assigned codes (see, e.g., the Philyaw patent at Col. 29, lines 48-62) does not teach or suggest a validation key including a random or pseudo-random number, as suggested by the Examiner in the final Office Action on page 6, line 12 – page 7, line 4.

We respectfully request that the final rejection of claim 24 be reversed.

Claims 10 – 17 and 19

Independent claim 10 reads as follows:

10. A method of authenticating permission to access a system comprising:

receiving a request to enter the system, the request including at least a validation key;

determining whether the validation key is valid, wherein the validation key comprises a time stamp and said determining determines whether the time stamp comprises a predetermined format; and

allowing access to the system based on a determination of said determining.

Claim 10 recites an act of determining whether a validation key is valid, wherein the validation key includes a time stamp and the determining determines whether the time stamp has a predetermined format.

By way of example only, page 16, paragraph 60, of the subject specification describes various different format determinations including, e.g., checking whether a validation key includes a proper amount of characters, is the right size, falls within a predetermined range, etc. Other examples include providing a time stamp to a format checker (e.g., a visual basic routine expecting to receive a date-time format or a process or software routine to determine valid time formats, etc.) to make a determination.

The Examiner cites[2] the Philyaw patent at Col. 31, lines 12-15, as teaching "determining whether the validation key is valid, wherein the validation key comprises a time stamp and said determining determines whether the time stamp comprises a predetermined format." The Examiner suggests that such an act is ***inherently*** taught at the cited passages. We respectfully disagree.

The cited passage at Col. 31, lines 12-15 focuses on a time the VEMP 3002 was received ("...evaluating the supplemental validation data 3006 for time stamp information ***relating to the time the UEMP was received at the reference computer***.") (emphasis added).

This teaching is unconcerned with a time stamp **format**. Perhaps this is so because the system can handle multiple different formats? We are left to guess because the cited passage just doesn't say. What it does say, however, is that the focus is on time information (e.g., received at 6:12 am) – and not on a format of the time stamp (e.g., size, expected characters, type or format, etc.). Indeed, there is no teaching or suggestion that a time stamp format is even the slightest bit important in the Philyaw patent.

In contrast, claim 10 recites that a determination is made based on the time stamp information, e.g., through checking whether a validation key includes a proper amount of characters, is the right size, falls within a predetermined range, analysis by a software routine expecting to receive a date-time format or a process or software routine to determine valid time formats, etc.

We respectfully request that the final rejection of claim 10 be reversed.

---

2 See page 5, lines 15-25 of the June 2, 2005 final Office Action.

Claims 20 - 23

Independent claim 20 reads as follows:

20. A method of authenticating permission to access a system via the internet, said method comprising:

receiving a request to enter the system, the request including at least a validation key;

determining whether the validation key has been previously received; and

allowing access to the system based on a determination of said determining.

Claim 20 recites determining whether a received validation key has been previously received, and allowing access to a system based on a determination of whether the validation key has been previously received.

By way of example only, and with reference to the subject specification at paragraphs 61 and 62 on pages 16 and 17, received validation keys may be stored in a database, list, table or data record, etc. The database, etc. may be refreshed on occasion as well. When a validation key is received, the database is queried to determine whether the received validation key has been previously received or received within a predetermined time.

The Examiner cites[3] numerous passages of the Philyaw patent to teach "determining whether the validation key has been previously received; and allowing access to the system based on a determination of said determining." We respectfully disagree with the Examiner's interpretation of these passages.

The cited passages in the Philyaw patent seemed concerned with user information. In fact, an important motive of the contest discussed in the Philyaw patent is collecting user information including viewing or buying habits of a user (*please see* the Philyaw patent at Col. 29, lines 19-21).

---

3 See the final Office Action on page 2, starting at paragraph 3 through page 3. The citations to the Philyaw patent include Col. 29, lines 19-47; Col. 28, lines 64-6; Col. 30, lines 34-44; and Col. 31, lines 2-5. We also note that the final Office Action appears to have a typo on line 3 of

The cited Col. 31, lines 2-5 passage is concerned about whether there is a minimum amount of user data included in a VEMP 3002 (see lines 2-6). But this is not a determination based on whether a validation key – itself -- has been previously received; but, rather, a determination of whether there is sufficient user information or user registration. The fact that a VEMP 3002 might correspond in some way to user information or user registration information does not teach or suggest that the VEMP 3002 – itself -- has been previously received.

The Philyaw patent does describes a process for determining whether a received VEMP 3002 constitutes a valid entry (*please see* Col. 31, lines 29-35). A VEMP 3002 is assigned a sequential number when received, with the sequential number being compared to a predetermined range of numbers (*please see* Col. 31, lines 29-35). Thus, the system discussed at the cited passages of the Philyaw patent is not understood to determine whether the VEMP 3002 has been previously received.

We also disagree with the Examiner's ***inference*** that a user is entitled to only one contest entry (*please see* the final Office Action on page 3, lines 22-24). Recall that an important motivation for the contest is collecting intelligence on user habits (*please see* the Philyaw patent at Col. 29, lines 19-21). And there is also a contest example where a prize is awarded to a first user who scans an article exactly matching a selected article (*please see* the Philyaw patent at Col. 32, lines 1-4). This example includes a User 3 who scans the wrong article (*please see* the Philyaw patent at Col. 32, lines 10-19). The Examiner's ***inference*** would foreclose User 3 from trying again. This seems a poor contest model to us. Instead, it seems that the contest sponsors would encourage User 3 to try again so that they can capture additional information on the user's habits and encourage further contest participation.

Thus, we respectfully submit that the Examiner's inference is not soundly based.

And we respectfully request that the final rejection of claim 20 be reversed.

---

paragraph 3. We believe "claim 10" should read --claim 20--.

Claims 31 - 37

Independent claim 31 reads as follows:

31. A method of operating a computer server, the computer server to communicate with at least one user terminal, said method comprising:

receiving an identifier from the user terminal;

identifying a pointer associated with the identifier;

determining whether the pointer is a predetermined class, and

if not the predetermined class, communicating the pointer to the user terminal; and

if the predetermined class, generating a validation key, and communicating the pointer and validation key to the user terminal.

One of many implementations covered by claim 31 is discussed in paragraphs 47 and 48 of the subject specification. Upon receipt of an identifier (or message), server 18 (Fig. 7) queries an associated database to retrieve a corresponding pointer, e.g., a URL or IP address (step S40, Fig. 8). In step S42, it is determined whether the pointer is associated with a predetermined class, e.g., is the pointer associated with a restricted-access or exclusive website. If access is not restricted, the pointer is communicated to the user terminal 16 in step S44. If access is restricted, a validation key is determined (and optionally encoded) in step S46. The pointer and validation key are communicated to the user terminal in step S48.

Restricted access or exclusivity can be identified in a number of ways. For example, one way is to set a flag or store another parameter with the pointer to indicate such status. The server (or software running on such) then checks the flag or parameter to determine exclusivity. Another way is to store exclusive or restricted pointers in a list, database, table, etc. When a pointer is selected in response to a received identifier, the server 18 (or software running on such) then determines whether the selected pointer is listed in the list, database or table. If the pointer is listed it is determined to be exclusive or restricted. Additional techniques will be covered by this claim as well.

The final Office Action cites[4] the Philyaw patent at Col. 28, lines 11-22 as teaching: "identifying a pointer associated with an identifier."

But there doesn't seem to be any sort of identifying a pointer (e.g., a URL or IP address) with the identifier at this cited passage. If, for example, the "identifier" is an UEMP as suggested by the Examiner, where then is there an act of identifying a pointer associated with the UEMP? Instead of identifying a pointer associated with the UEMP, the cited passage of the Philyaw patent forwards the UEMP to a reference computer.

The final Office Action cites[5] the Philyaw patent at Col. 29, line 19 - Col. 30, line 6 as teaching: "determining whether the pointer is a predetermined class."

There seems to be some confusion in the office action regarding a pointer. The final Office Action first tries to establish that the UEMP corresponds to the "identifier" recited in claim 31 as discussed above. But then the final Office Action suggests that the UEMP is a pointer. Recall, however, that there is a pointer (e.g., an URL, IP address or web address) identified. But instead of determining whether a pointer is of a predetermined class, the Office Action tries to show a determination of whether the UEMP is of a predetermined class. *Please see* the final Office Action at page 4, line 21 – page 5, line 2.

The Examiner's position in the final Office Action misses the point. Claim 31 is concerned with determining whether a pointer (e.g., a web site address) is of a particular class, and not whether the identifier (or UEMP as stated by the Examiner) is of a particular class. For example, claim 31 would determine whether a website is an exclusive website or is otherwise restricted.

To be clear, a pointer (or "routing information") is discussed in the Philyaw patent. *Please see*, e.g., the discussion involving a RMP 2802 that includes "routing information" at Col.

---

4 See the final Office Action at page 4, lines 11-13.

5 See the final Office Action at page 4, lines 21-22.

30, lines 24-26. But this routing information is not analyzed to determine whether it is of a particular class, and different acts of communicating are not carried out based on whether the *routing information* falls within a predetermined class.

Determining whether a user code 2606 has a particular validity status, as suggested in the final Office Action, is not helpful to teach or suggest determining whether the pointer is of a predetermined class. If anything, determining a validity status of a user codes suggests determining whether an identifier (or UEMP as suggested by the Examiner) is a particular class. For example, the user code 2606 carried by the UEMP 2602 is either valid or it is not. Please see, Col. 29, line 58 – Col. 30, line 6.

Thus, we respectfully request that the final rejection of claim 31 be reversed.

Claim 38

Independent claim 38 reads as follows:

A computer server, said computer server to communicate with at least one user terminal, said computer server comprising:

means for receiving an identifier from the user terminal;

means for identifying a pointer associated with the identifier;

means for determining whether the pointer is a predetermined class, and

if not the predetermined class, means for communicating the pointer to the user terminal; and

if the predetermined class, means for generating a validation key, and communicating the pointer and validation key to the user terminal.

As discussed above with respect to claim 31, there appears to be some confusion regarding the separate nature of an identifier and a pointer. The final Office Action seems to impermissibly blurs these lines.

Claim 38 recites means to determine whether a pointer (e.g., a URL or IP address) is of a predetermined class.

A pointer (or "routing information") is discussed in the Philyaw patent. Please see, e.g., the discussion involving a RMP 2802 that includes "routing information" at Col. 30, lines 24-26. But this routing information is not analyzed to determine whether it is of a particular class, and different acts of communicating are not carried out based on whether the *routing information* falls within a predetermined class.

And determining whether a user code 2606 has a particular validity status is not helpful to teach or suggest determining whether the pointer is of a predetermined class. If anything, this suggests determining whether an identifier (or UEMP as suggested by the Examiner) is a particular class. For example, the user code 2606 carried by the UEMP 2602 is either valid or it is not. Please see, Col. 29, line 58 – Col. 30, line 6.

We respectfully request that the final rejection of claim 38 be reversed.

Claims 1 – 4, 8 and 9

Independent claim 1 reads as follows:

1. A method of regulating access to a website by a user terminal via the internet, the user terminal reading a document including an embedded digital watermark, said method comprising:

at the user terminal, extracting identifying data from the digital watermark, and providing the identifying data to a central computer;

at the central computer:

identifying a pointer associated with the identifying data;

generating a validation key;

encoding the validation key through at least one of i) hashing, ii) rotating and iii) converting the validation key to alpha-characters and then adjusting the characters according to a code key; and

providing the pointer and the validation key to the user terminal;

at the user terminal, communicating with the website via the pointer and providing the validation key to the website; and

at the website, regulating access to the website by the user terminal based at least

in part on the validation key.

Claim 1 recites, in combination with other features of the claim, that the central server encodes the validation key through at least one of i) hashing, ii) rotating and iii) converting the validation key to alpha-characters and then adjusting the characters according to a code key.

The final Office Action cites Col. 30, lines 10-14 as teaching these features. *Please see* the final Office Action at page 6, lines 1-11.

But we respectfully disagree.

The encoding in claim 1 must be at least one of: i) hashing, ii) rotating and iii) converting the validation key to alpha-characters and then adjusting the characters according to a code key. The Examiner makes vague reference to what is known in the art relative to the cited passage.

But the cited passage specifically calls out encryption. Encryption seems to teach away from hashing a number (e.g., creating a reduce-bit representation of the number), rotating (e.g., a circular rotation) and converting to alpha-characters and adjusting the characters according to a key.

We respectfully request that the final rejection of claim 1 be reversed.

CONCLUSION AND REQUEST FOR REVERSAL

The Philyaw patent fails to disclose all of the limitations of the pending claims. (Other deficiencies of the Philyaw patent need not be further belabored at this time.) As such, the claims are believed patentable over the Philyaw patent.

Appellants respectfully request that the Board reverse the final rejection of the pending claims.

Respectfully submitted,

Date: November 29, 2005

DIGIMARC CORPORATION

Customer No. 23735

By _____

Steven W. Stewart
Registration No. 45,133

Telephone: 503-469-4685
FAX: 503-469-4777

CLAIMS APPENDIX

1. (previously presented): A method of regulating access to a website by a user terminal via the internet, the user terminal reading a document including an embedded digital watermark, said method comprising:

at the user terminal, extracting identifying data from the digital watermark, and providing the identifying data to a central computer;

at the central computer:

identifying a pointer associated with the identifying data;

generating a validation key;

encoding the validation key through at least one of i) hashing, ii) rotating and iii) converting the validation key to alpha-characters and then adjusting the characters according to a code key; and

providing the pointer and the validation key to the user terminal;

at the user terminal, communicating with the website via the pointer and providing the validation key to the website; and

at the website, regulating access to the website by the user terminal based at least in part on the validation key.

2. (original): The method according to claim 1, wherein the identifying data comprises a document identifier.

3. (original): The method according to claim 2, wherein the pointer comprises at least one of a URL, IP address and web address.

4. (original): The method according to claim 2, wherein the validation key comprises a date-time value.

5 – 7. canceled.

8. (previously presented): The method according to claim 1 further comprising encoding the code key with the validation key.

9. (original): The method according to claim 1, wherein the validation key comprises at least one of a predetermined number and a pseudo-random number.

10. (previously presented): A method of authenticating permission to access a system comprising:

receiving a request to enter the system, the request including at least a validation key;

determining whether the validation key is valid, wherein the validation key comprises a time stamp and said determining determines whether the time stamp comprises a predetermined format; and

allowing access to the system based on a determination of said determining.

11. (original): The method according to claim 10, wherein said system comprises a website.

12. (previously presented): The method according to claim 10, further comprising decoding the validation key.

13. (previously presented): The method according to claim 10, wherein said determining further determines whether the timestamp is stale.

14. (previously presented): The method according to claim 10, said determining further determines whether the timestamp is within a predetermined range.

15. (previously presented): The method according to claim 10, wherein the validation key comprises a predetermined number, and said determining determines whether the predetermined number matches at least one number on a list of numbers.

16. (original): The method according to claim 10, wherein the system provides information related to a digitally watermarked document.

17. (previously presented): The method according to claim 10, further comprising determining whether the validation key comprises a valid value.

18. canceled.

19. (original): The method according to claim 10, wherein the request includes a URL and the validation key is appended to the URL.

20. (previously presented): A method of authenticating permission to access a system via the internet, said method comprising:

receiving a request to enter the system, the request including at least a validation key;

determining whether the validation key has been previously received; and

allowing access to the system based on a determination of said determining.

21. (original): The method according to claim 20, wherein the validation key includes at least one of a date-time value, a pseudo-random number and a predetermined number.

22. (previously presented): The method according to claim 21, wherein said determining comprises querying a database to determine if the validation key is stored therein.

23. (original): A method according to claim 21, further wherein the request comprises a URL identified from a digitally watermark-based system.

24. (previously presented): A system for exchanging data comprising:

a central server comprising at least one database including pointer information, wherein when a user terminal communicates an extracted watermark identifier to said central server, said central server identifies a corresponding pointer associated with the extracted watermark identifier, and wherein said central server generates a validation key including at least one of a random and pseudo-random number, and encodes the validation key, and wherein said central server appends the validation key to the corresponding pointer, and communicates the pointer and validation key to the user terminal.

25. (original): The system according to claim 24, wherein the pointer comprises at least one of a URL, IP address and web address.

26. (previously presented): The system according to claim 25, wherein the validation key further comprises a date-time value.

27. (original): The system according to claim 24, wherein said central server encodes by at least one of hashing, encrypting, and rotating.

28. (original): The system according to claim 27, wherein the central server encodes by converting the validation key to alpha-characters, and adjusting the characters according to a code key.

29. (original): The system according to claim 28, wherein the central server encodes the code key with the validation key.

30. canceled.

31. (previously presented): A method of operating a computer server, the computer server to communicate with at least one user terminal, said method comprising:

receiving an identifier from the user terminal;

identifying a pointer associated with the identifier;

determining whether the pointer is a predetermined class, and

if not the predetermined class, communicating the pointer to the user terminal; and

if the predetermined class, generating a validation key, and communicating the pointer and validation key to the user terminal.

32. (original): The method according to claim 31, wherein the pointer comprises at least one of a URL, IP address and web address.

33. (original): The method according to claim 32, wherein the predetermined class comprises at least one of a restricted access website, exclusive access website, an entry-through-purchased documents website, a restricted URL, and an exclusive URL.

34. (original): The method according to claim 33, wherein the validation key comprises at least one of a time stamp, a predetermined number, and a pseudo-random number.

35. (original): The method according to claim 34, wherein said document identifier comprises an identifier extracted from a digitally watermarked document.

36. (previously presented): The method according to claim 35, further comprising encoding the validation key.

37. (original): The method according to claim 34, wherein said document identifier comprises an identifier extracted from a digitally watermarked document.

38. (previously presented): A computer server, said computer server to communicate with at least one user terminal, said computer server comprising:

means for receiving an identifier from the user terminal;

means for identifying a pointer associated with the identifier;

means for determining whether the pointer is a predetermined class, and

if not the predetermined class, means for communicating the pointer to the user terminal; and

if the predetermined class, means for generating a validation key, and communicating the pointer and validation key to the user terminal.

EVIDENCE APPENDIX

(No Evidence)

RELATED PROCEEDINGS APPENDIX

(No Related Proceedings)